非可換な代数構造に基づく暗号系の研究

修士学位論文要約（平成30年３月）

非可換な代数構造に基づく暗号系の研究

須田 厚
指導教員: 静谷 啓樹　学位論文指導教員: 小泉 英介

Cryptosystems Based on Non-Commutative Algebraic Structure

Atsushi SUDA
Supervisor: Hiroki SHIZUYA　Research advisor: Eisuke KOIZUMI

Non-commutative cryptography a candidate for post-quantum cryptographic schemes. There have been proposed several non-commutative schemes so far. However, many of them lack rigorous security proofs or their security depends on some commutative structure that are vulnerable against quantum computer's attack. In this thesis, we propose an encryption scheme, and give a rigorous security proof based on the conjugacy problem over nonabelian groups.

1　はじめに

現在までに考えられている暗号方式の多くは, その安全性を素因数分解問題や離散対数問題に依存している. 一方で, Shor[4] により, これらの問題を量子計算機で効率的に解くアルゴリズムが発見されている. そのため, 量子計算機の実用化により, これらの問題に依存する暗号方式は, その安全性を失う.

量子計算機が実用化されても安全性が保たれると考えられている暗号方式の一つに, 非可換な群や環を利用した暗号方式がある. 非可換な群や環を利用した暗号方式は数多く提案されているが, 安全性証明の与えられていないものも少なくない. これでは方式自体の安全性に疑問が残るため, そのまま実用化することはできない. また, その仕組みの中で何らかの可換性を利用している暗号方式も存在する. この可換性は, 方式の安全性の根拠となる部分で, また, 従来の可換群上の暗号方式の仕組みに類似する機能を実現するために利用されることが多い. このため, 可換群上の問題を解くためのアルゴリズムおよびその変形などにより, 暗号方式の安全性が失われる可能性がある. そこで, 本研究では以下の条件をみたす具体的な暗号方式の構成を目指す:

- 非可換群上の問題の困難性を仮定することにより, 安全性証明を与えることができる.
- 安全性の根拠となる部分に可換性を利用しない.

これを実現するため, Diffie-Hellman 鍵共有方式 [3] を利用して IND-CCA 安全な暗号方式を構成した Cramer と Shoup の方法論 [2] を可換版構成法と位置付け, それと並行的な議論として非可換版を展開する. 具体的には, Anshel らが提案した非可換群上の鍵共有方式 [1] を基にして暗号方式を構成する. そして, 構成した暗号方式に対して安全性の証明を行う.

2　本論文の結果

最初に, 語 (word) と呼ばれる概念を定義する.

X_n を n 個の元 $x_1, \ldots, x_n$ から成る集合とする. 各 $x \in X_n$ に対して x^{-1} という元を考え $X_n^{-1} := \{x^{-1} \mid x \in X_n\}$, $X_n^{\pm 1} := X_n \cup X_n^{-1}$ とおく.

$X_n^{\pm 1}$ の元を文字といい, 文字を任意の順序に有限個並べた列 $w(X_n) = w_1 \cdots w_l$ $(w_i \in X_n^{\pm 1})$ を X_n 上の語という. また, l を w の長さという. 長さ l 以下の X_n 上の語の集合を $W(X_n; l)$ とする.

G を群, $S = \{s_1, \ldots, s_n\} \subseteq G$ を n 個の元からなる G の部分集合とする. このとき, X_n 上の語 $w(X_n)$ の各 x_i に s_i を, x_i^{-1} に s_i^{-1} を代入することで G の元が定まる. この元のことを $w(S)$ と書く. また, $a, b \in G$ に対して $aSb := \{as_1b, \ldots, as_nb\}$ と定義する. 簡単な計算により, 任意の $a \in G$ と X_n 上の語 w に対して $w(a^{-1}Sa) = a^{-1}w(S)a$ が成り立つ.

次に群生成アルゴリズムを定義する.

群生成アルゴリズム GenG**：** 1^k を入力として以下の性質をみたす組 $(G, p, \widetilde{p}, S_1, w_{s_{2,1}}, \ldots, w_{s_{2,p(k)}}, \mathrm{H})$ をランダムに出力する：

1. G は位数 $\mathsf{ord}(G) = \Omega(2^k)$ の非可換群である.
2. p と $\widetilde{p}$ は k についての多項式.
3. $S_1 = \{s_1, \ldots, s_{p(k)}\} \subseteq G$ である.
4. $w_{s_{2,1}}, \ldots, w_{s_{2,p(k)}} \in W(X_{p(k)}; \widetilde{p}(k))$ である.
5. $\mathrm{H} : G^3 \to G$ はハッシュ関数で, 制限付き標的衝突困難性をみたす.

以上の準備のもとで, 本論文で構成した暗号方式 $\Sigma = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ を述べる.

鍵生成アルゴリズム KeyGen : 1^k を入力として以下を実行する.

K1. $\mathsf{GenG}(1^k)$ を実行する.
K2. $S_2 = \{w_{s_{2,1}}(S_1), \ldots, w_{s_{2,p(k)}}(S_1)\}$ とする.
K3. $w_{x_1}, w_{x_2}, w_{y_1}, w_{y_2}, w_{z_1}, w_{z_2} \xleftarrow{U} W(X_{p(k)}; \widetilde{p}(k))$ を選び, $x_1 = w_{x_1}(S_1)$, $x_2 = w_{x_2}(S_2)$, $y_1 = w_{y_1}(S_1)$, $y_2 = w_{y_2}(S_2)$, $z_1 = w_{z_1}(S_1)$, $z_2 = w_{z_2}(S_2)$ を計算する.
K4. $X = x_2^{-1}x_1^{-1}S_1x_1x_2$, $Y = y_2^{-1}y_1^{-1}S_1y_1y_2$, $Z = z_2^{-1}z_1^{-1}S_1z_1z_2$ とする.
K5. 公開鍵を $pk = (G, S_1, S_2, X, Y, Z, \mathrm{H})$, 秘密鍵を

$$sk = (x_1, x_2, y_1, y_2, z_1, z_2, w_{x_1}, w_{x_2}, w_{y_1}, w_{y_2}, w_{z_1}, w_{z_2})$$

として, (pk, sk) を出力する.

暗号化アルゴリズム Enc : 公開鍵 pk と平文 $m \in G$ を入力として以下を実行する.

E1. $w_r \xleftarrow{U} W(X_{p(k)}; \widetilde{p}(k))$ を選び, $r = w_r(S_1)$ を計算する.
E2. $R_1 = r^{-1}S_1r = \{r_{1,1}, \ldots, r_{1,p(k)}\}$ とする
E3. $R_2 = r^{-1}S_2r = \{r_{2,1}, \ldots, r_{2,p(k)}\}$ とする.
E4. $a = w_r(Z)$ と $c = mr^{-1}a$ を計算する.
E5. $u_1 = r_{1,1} \cdots r_{1,p(k)}$ と $u_2 = r_{2,1} \cdots r_{2,p(k)}$, $\alpha = \mathrm{H}(u_1, u_2, c)$ を計算する.
E6. $b = w_r(X)$ と $d = w_r(Y)$ を計算する.
E7. $v_1 = b^{-1}r$, $v_2 = d^{-1}r\alpha$, $v = v_1v_2$ を計算する.
E8. $C = (R_1, R_2, c, v)$ を暗号文として出力する.

復号アルゴリズム Dec : 公開鍵 pk , 秘密鍵 sk と暗号文 $\widehat{C} = (\widehat{R}_1, \widehat{R}_2, \widehat{c}, \widehat{v})$ を入力として以下を実行する. ここで

$$\widehat{R}_1 = \{\widehat{r}_{1,1}, \ldots, \widehat{r}_{1,p(k)}\}, \widehat{R}_2 = \{\widehat{r}_{2,1}, \ldots, \widehat{r}_{2,p(k)}\}$$

とする.

D1. $\widehat{R}_1, \widehat{R}_2 \in G^{p(k)}$ かどうか, また $\widehat{c}, \widehat{v} \in G$ かどうか確認する. 違うなら $\perp$ を出力する.
D2. $\widehat{u}_1 = \widehat{r}_{1,1} \cdots \widehat{r}_{1,p(k)}$ と $\widehat{u}_2 = \widehat{r}_{2,1} \cdots \widehat{r}_{2,p(k)}$, $\widehat{\alpha} = \mathrm{H}(\widehat{u}_1, \widehat{u}_2, \widehat{c})$ を計算する.
D3. $e = w_{x_1}(\widehat{R}_1)w_{x_2}(\widehat{R}_2)$ と $f = w_{y_1}(\widehat{R}_1)w_{y_2}(\widehat{R}_2)$ を計算する.
D4. $\widehat{v}_1 = x_2^{-1}x_1^{-1}e$ と $\widehat{v}_2 = y_2^{-1}y_1^{-1}f\widehat{\alpha}$ を計算する.
D5. $\widehat{v} = \widehat{v}_1\widehat{v}_2$ かどうか確認する. 違うなら $\perp$ を出力する.
D6. $h = w_{z_1}(\widehat{R}_1)w_{z_2}(\widehat{R}_2)$ と $\widehat{m} = \widehat{c}z_2^{-1}z_1^{-1}h$ を計算する.
D7. $\widehat{m}$ を復号結果として出力する.

主定理
共役判定仮定および同時共役判定仮定が成立するならば, 提案方式 Σ は IND-rCCA 安全である.

3 まとめ

非可換群において以下の条件をみたす公開鍵暗号方式の構成を目指した:

- 非可換群上の問題の困難性を仮定することにより, 安全性証明を与えることができる.
- 安全性の根拠となる部分に可換性を利用しない.

そして, 非可換群上の鍵共有方式である AAG 鍵共有方式を基に暗号方式の構成を提案し, その暗号方式は, 共役判定問題および同時共役判定問題がどちらも困難という仮定の下で IND-rCCA 安全であることを証明した.

ただしこの rCCA という攻撃では, 攻撃者が復号オラクルに問い合わせる暗号文の形式に一定の制限がかけられている. そのため, 暗号方式にとって一般的に望ましいとされる IND-CCA 安全と比較すると, 本論文で証明した安全性はやや弱い. この制限を除去することが改善策として今後の課題である.

文献

[1] I. Anshel, M. Anshel, D. Goldfeld. “An algebraic method for public-key cryptography.” Math. Res. Lett. Vol.6, No.3, pp.287–291, 1999.

[2] R. Cramer, V. Shoup. “A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack.” Advances in Cryptology - CRYPTO ’98, pp. 13–25, 1998.

[3] W. Diffie, M. E. Hellman. “New direction in cryptography.” IEEE Trans. Inform. Theory, Vol.IT-22, No.6, pp.644–654, 1976.

[4] P. W. Shor. “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.” SIAM J. Comput. Vol.26, No.5, pp.1484–1509, 1997.